

Multi-Factor Authentication

Frequently Asked Questions (FAQs)

The University of Canterbury (UC) has enabled Multi-Factor Authentication (MFA) for all UC Microsoft 365 applications (e.g., Outlook, Word, Excel, OneDrive, PowerPoint, SharePoint, Teams) as well as other applications that use your UC Microsoft login.

Who will need to use MFA?

All accounts at UC including students, staff, visitors, and alumni, are required to have their accounts protected with MFA.

What is MFA?

MFA is a quick, easy way to confirm your identity when logging into online services such as Microsoft 365, banking, social media accounts, and even online grocery shopping.

MFA uses a second method of authentication alongside your password to ensure it's you logging in to your account. This 'second check' confirms that you are who you say you are and can be done through the below recommended methods:

- **Passkey in Microsoft Authenticator** (available on iOS and Android)
 - Officially supported by the UC Service Desk
 - Enables passwordless login
 - Requires Android 10 or iOS 16+
 - Allows the use of biometrics (face, fingerprint)
 - Strong phishing resistance
- **Physical passkey** (YubiKey 5 NFC, 5C NFC, and 5C Nano)
 - Strong phishing-resistant authentication
 - Works offline and doesn't require a mobile device
- **Passkey in 1Password**
 - Allows for a seamless login via the browser extension
 - Works across many platforms including web browsers
 - No separate device needed
- **An authentication app of your choice**
 - Such as Apple Passwords or Google Authenticator

What applications require MFA?

All UC Microsoft 365 applications will require MFA, such as Outlook, Teams, OneDrive, Word, Excel, SharePoint, Forms and PowerPoint. We also have many other applications that use your UC Microsoft account to sign in, these also will have similar security standards applied.

What are my authentication options?

You can choose up to four methods; we recommend using one primary and one backup method.

In order of preference and level of security:

- Passkey in Microsoft Authenticator
- Passkey
- Notification or number matching through Microsoft Authenticator
- Time-based One-Time Password (TOTP) from an authenticator app

Why are we doing this?

Every week, numerous threat actors attempt to compromise UC accounts through methods such as phishing emails and password-spray attacks. MFA establishes a second line of defence, ensuring cybercriminals will require more than just an email and password to access your account.

How often will I need to use MFA?

You will be asked to MFA when you access any of your UC Microsoft 365 applications or other applications that use your UC Microsoft account.

If you use the web browser to access your M365 account (such as www.office.com) you may be asked more frequently depending on your local browser settings.

Why am I being re-prompted for MFA regularly?

There are scenarios where users may be re-prompted for MFA if they:

- Sign out and sign in again to any Microsoft 365 apps
- Don't logon for an extended period
- Use multiple different devices
- Swap between multiple accounts (such as a personal account and your UC student account)
- Use multiple different web browsers (such as Chrome and Firefox)
- Unexpected activity is detected (such as sign-in from another country)

What is a Risky sign-in?

You may also be asked to MFA if risky sign-in activity is detected on your account.

Such scenarios could include; when you're accessing Microsoft 365 on a new or different device, or your credentials have been reported as, or have been, compromised.

Do I have to use the Microsoft Authenticator app? What are the alternatives?

You could use other authenticator apps such as Ente Auth, Google Authenticator, or Apple Passwords.

Please note that the Microsoft Authenticator app is the only application supported by the IT Service Desk should you encounter any issues that require technical assistance.

Can I opt-out of MFA?

No, all UC accounts including staff, students, visitors, and alumni UC accounts are required to be protected with MFA. This is a measure to protect you against unauthorised access to your UC account.

I do not own or regularly use a mobile phone, or I do not want to use my mobile phone

No problem at all! You're welcome to use any passkey or TOTP-based authentication method that works on your preferred device. Some examples of same-device authentication:

- Windows Hello (only available on Windows computers)
- Apple Passwords (only available on macOS and iOS)
- YubiKey (a physical security key)

If you're using a UC-managed computer, keep in mind that some apps may not be installable or available due to system restrictions.

What happens when I sign in using MFA?

Your experience will differ depending on what you choose to use as your MFA method; please see below for an expected experience of each method listed assuming you on your own PC and have signed into it before.

First, you'll need to sign into an application with your UC Microsoft.

1 Password via the browser extension

1. Select your username from the drop-down menu
2. Select sign in

Passkey in Microsoft Authenticator on your phone

1. It will prompt you to scan a QR code
2. With your phone, open the Microsoft Authenticator app
3. Scan the QR code on screen

An authentication app number matching/push notification

1. Type in your username and password
2. A push notification with a message such as: 'approve/deny' appears on your smartphone
3. Tap "approve"

A Time-based One-Time Password via an authenticator app

1. Enter your username and password
2. Open the authenticator app on your smartphone
3. Select your University of Canterbury account
4. Find the one-time password (time-sensitive)
5. Enter the one-time password in the box provided on the sign-in page.

Privacy questions

Please see the privacy considerations FAQ section on our webpage.

What do I do if I can't get into my account? Or I have lost my phone. Or I have left my phone at home. Or I don't have my mobile device with me.

This happens. Please get in touch with the IT Service Desk on 03 369 5000 or 0508 824 843 (after hours). If you are unable to use a phone:

Students

- Go to Te Pātaka, Student Services Hub, located in the centre of Ilam campus on levels 2 and 3 in Puaka-James Hight Central Library for in-person help, or to use a phone to call the IT Service Desk.

Staff

- Go to Matariki, Ground Floor, for in-person help (10am – 4pm, Mon-Fri).

Why is the Authenticator app more secure?

The primary reason is that it is easier for a hacker to gain physical access to your mobile phone. It is very easy to perform SIM swapping (stealing your phone number) and intercept any incoming SMS text messages, or phone calls received for authentication. With the Authenticator App, the codes are generated and stored temporarily on your phone (or another device) and expire within a specific timeframe.

What should I do if I receive a verification request, but I am not trying to sign in?

This may be an unauthorised access attempt, and we recommend that you decline the request and contact the service desk.

What if I travel frequently or am regularly on field trips?

What should I do if I don't have mobile data or good cellular service?

We recommend setting up the Microsoft Authenticator app and using a passkey on multiple devices, and TOTP as backup if needed, this way you can be sure to gain access even without service.

Please remember that to be able to access your UC applications online; you will also need access to Wi-Fi/data.

How do I change my MFA settings?

You can always return to <https://aka.ms/mysecurityinfo> and change your MFA verification methods at any time.

We encourage you to use the Microsoft Authenticator app as your first option because it offers you convenience, reliability, and security. We also recommend setting up more than one verification method where possible.

What if I don't want to install an app on my phone or my phone doesn't have the capability?

You can use any of the options previously listed:

- Windows Hello (only available on Windows computers)
- Apple Passwords (only available on macOS and iOS)
- 1Password (both desktop app and browser extension)
- YubiKey (a physical security key)
- Third-party authentication application

How do I know if I have already registered or not?

You can check your MFA registration settings by visiting <https://aka.ms/mysecurityinfo> to see the verification options you have set up.

What happens if I get a new mobile phone? How do I register for MFA?

You can change your MFA details at any time via the page <https://aka.ms/mysecurityinfo>

How do I restore my Authenticator App to a new phone?

Microsoft Authenticator provides a backup and restores capability for accounts. To move your Microsoft MFA account to a new phone, follow these steps:

1. Open the app on your old phone
2. Tap the three dots at the top right
3. Tap “Settings”
4. Enable “Cloud backup” or “iCloud Backup”
5. On your new phone, install the Microsoft Authenticator app and log in to your account
6. Select “Begin Recovery”

Your account and its settings will be added to your new phone.

Are there any costs?

Microsoft Authenticator and similar applications use an extremely small amount of data to complete incoming requests, if any at all.